WELCOME

RECON

MODULE - 7 & 8

https://www.linkedin.com/in/hariprasaanth/

MODULE - 7

PHASES OF HACKING

https://www.linkedin.com/in/hariprasaanth/

PHASES OF HACKING

5 TYPES

> Reconnaissance
  -> Passive Recon
  -> Active Recon
> Scanning
> Gaining Access
> Maintaining Access
> Clearing Tracks

PHASES OF HACKING

1. RECONNAISSANCE

In military operations, reconnaissance or scouting is the exploration of an area by military forces to obtain information about enemy forces, terrain, and other activities. Recon is collecting information and knowing deeply about the target system. This data is the main street for the programmer to hack the target system. It involves Footprinting, Enumeration, and Scanning.

Types of Recon

- > Passive Recon
- > Active Recon

PHASES OF HACKING

PASSIVE

In passive reconnaissance, you rely on publicly available knowledge. It is the knowledge that you can access from publicly available resources without directly engaging with the target. Think of it like you are looking at target territory from afar without stepping foot on that territory.

- Checking job ads related to the target website.
- Reading news articles about the target company.
- Doing an OSINT

PHASES OF HACKING

ACTIVE

Active reconnaissance, on the other hand, cannot be achieved so discreetly. It requires direct engagement with the target. Think of it like you check the locks on the doors and windows, among other potential entry points.

> Connecting to one of the company servers
> Calling the company in an attempt to get information.
> Entering company premises pretending as someone

PHASES OF HACKING

2. SCANNING

Port scanning: This phase involves scanning the target for information like open ports, Live systems, and various services running on the host.

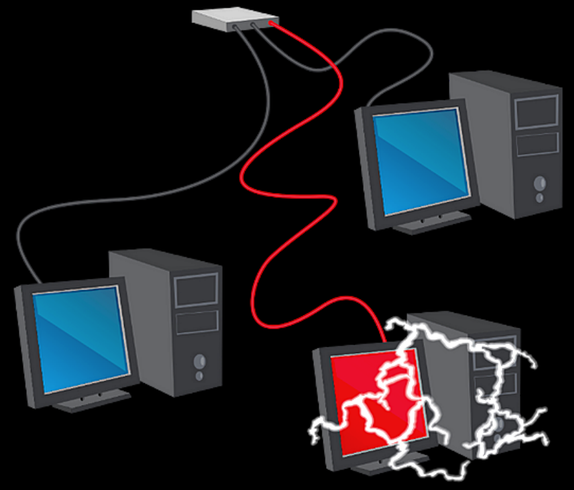
Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of the network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

PHASES OF HACKING

3. GAINING ACCESS

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.



PHASES OF HACKING

4. MAINTAINING ACCESS

Hacker may just hack the system to show it was vulnerable or they can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits, or other malicious files. The aim is to maintain access to the target until he finishes the tasks he planned to accomplish in that target.

PHASES OF HACKING

5. CLEARING TRACKS

No thief wants to get caught. An intelligent hacker always clears all evidence so that at a later point in time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

MODULE - 7

PASSIVE RECON

https://www.linkedin.com/in/hariprasaanth/

PASSIVE RECON

-> Check if the target is reachable.

$ ping annauniv.edu

-> Get the IP Address of the website.

$ ping annauniv.edu

$ host annauniv.edu

$ nslookup annauniv.edu

-> Gathering Registration records.

$ whois annauniv.edu

https://www.whois.com/whois/

-> Identifying technologies

$ whatweb annauniv.edu

Wappalyzzer browser extension

PASSIVE RECON

-> Perform DNS Analysis

https://dnsdumpster.com/

-> Perform Shodan Search

https://www.shodan.io/

-> Perform Mail Search

https://phonebook.cz/

-> Performing Username Search

https://whatsmyname.app/

-> Performing Satellite Search

https://earth.google.com/web/

PASSIVE RECON

-> Inspecting Old websites

https://archive.org/web/

-> Performing Google dorks

site:annauniv.edu

site:annauniv.edu inurl:computer

site:annauniv.edu intitle:computer

site:annauniv.edu filetype:pdf

person_name site:annauniv.edu

MODULE - 7

ACTIVE RECON

https://www.linkedin.com/in/hariprasaanth/

ACTIVE RECON

> Finding Subdomains

Install Golang

Install Assetfinder

```
$ assetfinder amazon.in
$ assetfinder amazon.in > out.txt
```

-> Taking Screenshot

Download Chrome

```
$ sudo su
$ dpkg -i name.deb

$ sudo apt update && sudo apt install google-chrome-stable
```

ACTIVE RECON

-> Download Aquatone

https://github.com/michenriksen/aquatone

```
$ unzip aquatone
$ sudo su
$ mv aquatone /usr/bin/
$ aquatone -version
$ cat out.txt | aquatone
```

-> Advanced Google dorks

https://github.com/IvanGlinkin/Fast-Google-Dorks-Scan

```
$ chmod +x FGDS.sh
$ ./FGDS.sh amazon.in
```

MODULE - 8

TESTING CMS

https://www.linkedin.com/in/hariprasaanth/

WORDPRESS

-> WPScan

https://github.com/wpscanteam/wpscan

https://wpscan.com/

WPScan WordPress security scanner. Written for security professionals and blog maintainers to test the security of their WordPress websites.

JOOMLA

-> joomscan

https://github.com/OWASP/joomscan

OWASP Joomla! Vulnerability Scanner (JoomScan) automates vulnerability detection and ensures reliability in Joomla CMS. Developed in Perl, it offers lightweight scanning with minimal impact. The tool detects offensive vulnerabilities, misconfigurations, and admin-level shortcomings, enhancing system security.

DRUPAL

-> drupwn

https://github.com/immunIT/drupwn

Drupwn can be run, using two seperate modes which are **enum** and **exploit**. The enum mode allows performing enumerations whereas the exploit mode allows checking and exploiting CVEs.

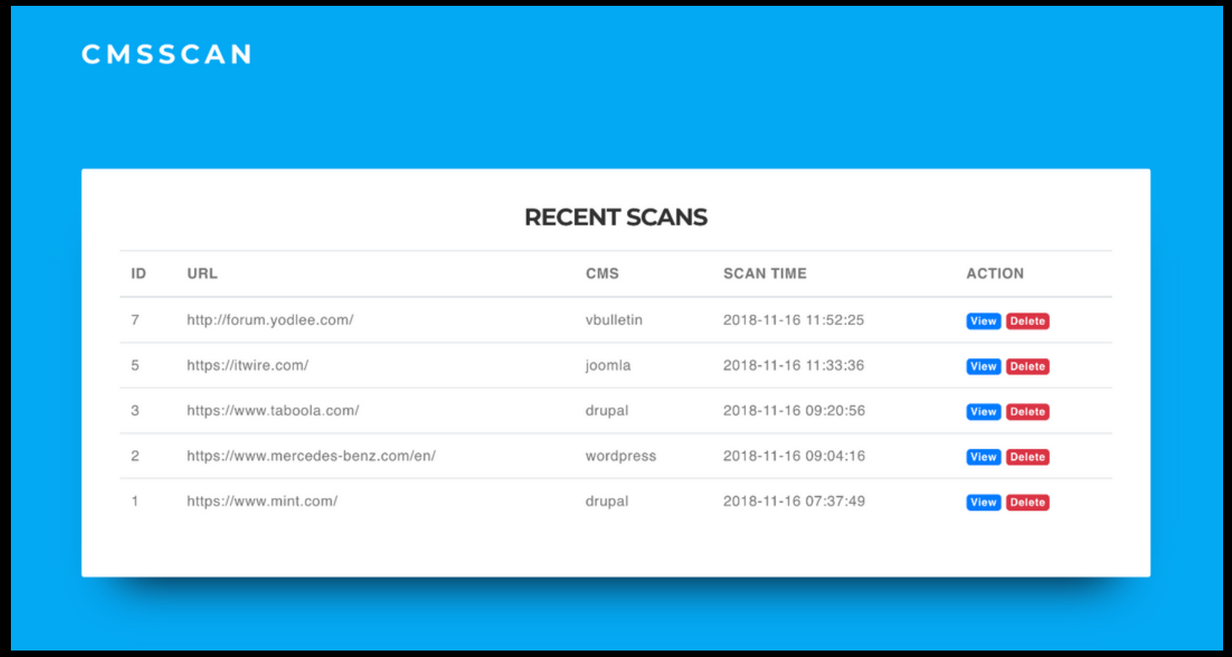
COMMON TOOLS

-> CMSmap

https://github.com/Dionach/CMSmap

-> CMSScan

https://github.com/ajinabraham/CMSScan



THANK YOU

THANK YOU

ANY QUERIES

https://www.linkedin.com/in/hariprasaanth/